UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,482	12/31/2003	Jeffrey J. Jonas	SVL920050503US2	9863

45729 7590 04/15/2009

GATES & COOPER LLP
6701 CENTER DRIVE WEST
SUITE 1050
LOS ANGELES, CA 90045

EXAMINER	
PATEL, NIRAV B	
ART UNIT	**PAPER NUMBER**
2435	
MAIL DATE	**DELIVERY MODE**
04/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/750,482	JONAS, JEFFREY J.	
	Examiner	Art Unit	
	NIRAV PATEL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2009 (RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's submission for RCE filed on Feb. 13, 2009 has been entered. Claims 1-58 are pending. Claims 1, 17, 30, 46 are amended by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 17, 21, 25, 30, 46, 50 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dulude et al. (US Patent No. 6,310,966) and in view Krawetz (US Pub. No. 2003/0084301).

As per claim 1, Dulude teaches:

receiving a first biometric data and a first personal key; processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a fist processed data comprised of the first biometric data and the first personal key in an irreversibly encrypted form (i.e. MD5 or one-way hash function) [Fig. 4 -- component 52 → a first hashed value, col. 6 lines 1-5, col. 5 lines 52-62]; receiving a second biometric data and a second personal key [Fig. 5 component 46, 50]; processing the second biometric data combined with the second personal key through

the irreversible cryptographic algorithm to form a second processed data comprised of the second biometric data and the second personal key in an irreversibly encrypted form (i.e. MD5 or one-way hash function) [Fig. 5 – component 78 → a second hashed value, col. 7 lines 7-14]; comparing the second processed data to the first processed data, without accessing the fist and second processed data in an unprocessed and unencrypted form in order to enable authentication of first and second biometric data and personal keys in a confidential manner [Fig. 5 – component 80, col. 7 lines 15-18]; and generating a signal pertaining to the comparison of the second processed data to the first processed data for use in an authentication process [Fig. 5, col. 7 lines 18-20].

Dulude teaches the authentication process without accessing the first and second processed data in an unprocessed and unencrypted form as above. Dulude doesn't expressively mention eliminating all storage or trace of unprocessed data prior to any comparison.

However, Krawetz teaches comparing the first processed data (verification signature) and the second processed data (check signature) for an authentication process [Fig. 3, paragraph 0023]. Further, Krawetz teaches eliminating all storage or trace of unprocessed and unencrypted data prior to any comparison [paragraph 0036 lines 10-15].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krawetz with Dulude, since one would have been motivated to protect the database of the server against susceptible to loss or theft of the data associated with a user [Krawetz, paragraph 0003, 0006].

Krawetz teaches the user data such as financial, personal or other type of sensitive or confidential information, and discarding or removing the unencrypted user data and identifier from the storage. However, Dulude teaches the user data includes the biometric data. Therefore, the combination of Dulude and Krawetz teaches eliminating all storage and trace of the biometric data and personal keys in an unprocessed form prior to any comparison.

As per claim 17, Dulude teaches:

receiving biometric data and personal key; processing the biometric data combined with the personal key through an irreversible cryptographic algorithm to form a processed data comprised of the first biometric data and the first personal key in an irreversibly encrypted form (i.e. MD5 or one-way hash function) [Fig. 4 -- component 52 → a first hashed value, col. 6 lines 1-5, col. 5 lines 52-62]; comparing the processed data to a secondary data, without accessing the fist and second processed data in an unprocessed and unencrypted form, in order to enable authentication of biometric data and personal key in a confidential manner [Fig. 5 – component 80, col. 7 lines 15-18].

Dulude teaches the authentication process without accessing the processed data in an unprocessed form as above. Dulude doesn't expressively mention eliminating all storage or trace of unprocessed data prior to any comparison.

However, Krawetz teaches comparing the processed data (verification signature) and the second data (check signature) for an authentication process [Fig. 3, paragraph

0023]. Further, Krawetz teaches eliminating all storage or trace of unprocessed and unencrypted data prior to any comparison [paragraph 0036 lines 10-15].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krawetz with Dulude, since one would have been motivated to protect the database of the server against susceptible to loss or theft of the data associated with a user [Krawetz, paragraph 0003, 0006].

Krawetz teaches the user data such as financial, personal or other type of sensitive or confidential information, and discarding or removing the unencrypted user data and identifier from the storage. However, Dulude teaches the user data includes the biometric data. Therefore, the combination of Dulude and Krawetz teaches eliminating all storage and trace of the biometric data and personal key in an unprocessed form prior to any comparison.

As per claim 21, the method of claim 17 wherein receiving the biometric data and the personal key occurs during an authentication process (Rejected per claim 1).

As per claim 25, the method of claim 17 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data (Rejected per claim 1).

As per claim 30, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 46, it encompasses limitations that are similar to limitations of claim 17. Thus, it is rejected with the same rationale applied against claim 17 above.

As per claim 50, The computer readable medium for performing the method of claim 46 wherein receiving the biometric data and the personal key occurs during an authentication process. (Rejected per claim 21.)

As per claim 54, The computer readable medium for performing the method of claim 46 further comprising generating a signal corresponding to the comparison of the processed data to the secondary data. (Rejected per claim 25.)

1. Claims 2-16, 18-20, 22-24, 26-29, 31-45, 47-49, 51-53, 55-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dulude et al. (US Patent No. 6,310,966) and in view in view Krawetz (US Pub. No. 2003/0084301) and in view of Musgrave et al. (US Patent No. 6,202,151).

As per claim 2, the rejection of claim 1 is incorporated and Musgrave teaches: generating a first variant from the first biometric data prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm. (Column 5, lines 15-19. The Examiner is interpreting concatenating the biometric with other data as to form a 'variant.')

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Musgrave with Dulude and Krawetz, since one would have been motivated to provide increased security and accuracy for authentication of electronic transaction [Musgrave, col. 3 lines 25-28].

As per claim 3, the rejection of claim 1 is incorporated and Musgrave teaches: generating a second variant from the second biometric data prior to processing the second biometric data and the second personal key through the irreversible cryptographic algorithm. (Column 5, lines 15-19 and Column 3, lines 54-57.)

As per claim 4, the rejection of claim 1 is incorporated and Musgrave teaches: processing the first biometric data through a secondary irreversible cryptographic algorithm prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm. (Column 3, lines 37-39)

As per claim 5, the rejection of claim 1 is incorporated and Musgrave teaches: adding salt to the first biometric data and the first personal key. (Figure 3, block 28. Musgrave et al. present a 'addition data to pad…[other] combined data,' per paragraph 15 of the applicant's specification. The Examiner is interpreting "User Input Data" given through device 28 as 'pad data' to pad 'Combined Data' that is biometric and public key data, as presented in both the reference and instant application.)

As per claim 6, the rejection of claim 1 is incorporated and Musgrave teaches: processing the first personal key through a cryptographic algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm. (Figure 3, blocks 32 and 34. The public key is processed with other data through the cryptographic hash algorithm 34.)

As per claim 7, the rejection of claim 1 is incorporated and Musgrave teaches: associating a first primary key to the first processed data. (Column 5, lines 45-60 and Column 6, lines 52-60. The Examiner is interpreting 'primary key' to be 'any personal inputted data' per paragraph 15 of the applicant's specification (e.g., a user inputted string). Therefore, one of the datum received in Musgrave et al., per block 28 of Figure 3, is a 'primary key.')

As per claim 8, the rejection of claim 1 is incorporated and Musgrave teaches: associating a second primary key to the second processed data. (Figure 3, block 36. Please note that the first set of data (primary key, personal key and biometric) in Musgrave et al. corresponds the second set of data in the instant application (e.g., enrollment data (all) is the "first" data in the instant application, but is called "second" in Musgrave et al.). Therefore, based on paragraph 8 of column 6, Figure 3, block 36 corresponds to both 1st and 2nd datum.)

As per claim 9, the rejection of claim 1 is incorporated and Musgrave teaches: receiving the first biometric data and the first personal key occurs during an enrollment process. (Column 6, lines 52-60.)

As per claim 10, the rejection of claim 1 is incorporated and Musgrave teaches: receiving the second biometric data and the second personal key occurs during an authentication process. (Column 3, lines 57-60.)

As per claim 11, the rejection of claim 1 is incorporated and Musgrave teaches: generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data. (Column 3, lines 49-63.)

As per claim 12, the rejection of claim 11 is incorporated and Musgrave teaches: issuing a confirmation signal allows access to a facility. (Column 6, lines 5-17.)

As per claim 13, the rejection of claim 11 is incorporated and Musgrave teaches: issuing a confirmation signal allows access to a system. (Column 6, lines 5-17.)

As per claim 14, the rejection of claim 1 is incorporated and Musgrave teaches: generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data. (Column 3, lines 49-63.)

As per claim 15, the rejection of claim 1 is incorporated and Musgrave teaches: storing the first processed data in a database. (Column 3, lines 49-63.)

As per claim 16, the rejection of claim 15 is incorporated and Musgrave teaches: the database includes a plurality of first processed data. (Column 3, lines 49-63.)

As per claim 18, the method of claim 17 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm (Rejected per claim 3).

As per claim 19, the method of claim 17 further comprising processing the biometric data through a secondary irreversible cryptographic algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm (Rejected per claim 4).

As per claim 20, the method of claim 17 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm (Rejected per claim 5).

As per claim 22, the method of claim 17 further comprising associating a primary key with the biometric data and the personal key (Rejected per claim 8).

As per claim 23, the method of claim 17 wherein the secondary data includes a secondary biometric data and a secondary personal key (Rejected per claim 1 and including the reasoning of claim 7).

As per claim 24, the method of claim 23 wherein the secondary biometric data and the secondary personal key is received during an enrollment process (Rejected per claim 23).

As per claim 26, the method of claim 25 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data (Rejected per claim 11).

As per claim 27, the method of claim 25 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data (Rejected per claim 14).

As per claim 28, the method of claim 25 wherein generating a signal allows entry into a facility when the processed data matches the secondary data (Rejected per claim 12).

As per claim 29, the method of claim 25 wherein generating a signal allows entry into a system when the processed data matches the secondary data (Rejected per claim 13).

As per claim 31 The computer readable medium for performing the method of claim 30 further comprising generating a first variant from the first biometric data prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm. (Rejected per claim 2.)

As per claim 32, The computer readable medium for performing the method of claim 30 further comprising generating a second variant from the second biometric data prior to processing the second biometric data and the second personal key through the irreversible cryptographic algorithm. (Rejected per claim 3.)

As per claim 33, The computer readable medium for performing the method of claim 30 further comprising processing the first biometric data through a secondary irreversible cryptographic algorithm prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm. (Rejected per claim 4.)

As per claim 34, The computer readable medium for performing the method of claim 30 further comprising adding salt to the first biometric data and the first personal key prior to processing the first biometric data and the second biometric data through the irreversible cryptographic algorithm. (Rejected per claim 5.)

As per claim 35, The computer readable medium for performing the method of claim 30 further comprising processing the first personal key through a reversible cryptographic

algorithm prior to processing the first biometric data and the first personal key through the irreversible cryptographic algorithm. (Rejected per claim 6.)

As per claim 36, The computer readable medium for performing the method of claim 30 further comprising associating a first primary key to the first processed data. (Rejected per claim 7.)

As per claim 37, The computer readable medium for performing the method of claim 30 further comprising associating a second primary key to the second processed data. (Rejected per claim 8.)

As per claim 38, The computer readable medium for performing the method of claim 30 wherein receiving the first biometric data and the first personal key occurs during an enrollment process. (Rejected per claim 9.)

As per claim 39, The computer readable medium for performing the method of claim 30 wherein receiving the second biometric data and the second personal key occurs during an authentication process. (Rejected per claim 10.)

As per claim 40, The computer readable medium for performing the method of claim 30 wherein generating a signal includes issuing a confirmation signal when the second processed data matches the first processed data. (Rejected per claim 11.)

As per claim 41, The computer readable medium for performing the method of claim 40 wherein issuing a confirmation signal allows access to a facility. (Rejected per claim 12.)

As per claim 42, The computer readable medium for performing the method of claim 40 wherein issuing a confirmation signal allows access to a system. (Rejected per claim 13.)

As per claim 43, The computer readable medium for performing the method of claim 30 wherein generating a signal includes issuing a rejection signal when the second processed data does not match the first processed data. (Rejected per claim 14.)

As per claim 44, The computer readable medium for performing the method of claim 30 further comprising storing the first processed data in a database. (Rejected per claim 15.)

As per claim 45, The computer readable medium for performing the method of claim 44 wherein the database includes a plurality of first processed data. (Rejected per claim 16.)

As per claim 47, The computer readable medium for performing the method of claim 46 further comprising generating a variant from the biometric data prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm. (Rejected per claim 18.)

As per claim 48, The computer readable medium for performing the method of claim 46 further comprising processing the biometric data through a secondary irreversible cryptographic algorithm prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm. (Rejected per claim 19.)

As per claim 49, The computer readable medium for performing the method of claim 46 further comprising adding salt to the biometric data and the personal key prior to processing the biometric data and the personal key through the irreversible cryptographic algorithm. (Rejected per claim 20.)

As per claim 51, The computer readable medium for performing the method of claim 46 further comprising associating a primary key with the biometric data and the personal key. (Rejected per claim 22.)

As per claim 52, The computer readable medium for performing the method of claim 46 wherein the secondary data includes a secondary biometric data and a secondary personal key. (Rejected per claim 23.)

As per claim 53, The computer readable medium for performing the method of claim 52 wherein the secondary biometric data and the secondary personal key is received during an enrollment process. (Rejected per claim 24.)

As per claim 55, The computer readable medium for performing the method of claim 54 wherein generating a signal includes issuing a confirmation message when the processed data matches at least a portion of secondary data. (Rejected per claim 26.)

As per claim 56, The computer readable medium for performing the method of claim 54 wherein generating a signal includes issuing a denial message when the processed data does not match at least a portion of secondary data. (Rejected per claim 27.)

As per claim 57, The computer readable medium for performing the method of claim 54 wherein generating a signal allows entry into a facility when the processed data matches the secondary data. (Rejected per claim 28.)

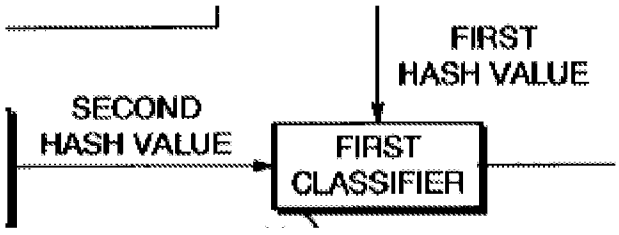
As per claim 58, The computer readable medium for performing the method of claim 54 wherein generating a signal allows entry into a system when the processed data matches the secondary data. (Rejected per claim 29.)

Response to Arguments

3. Applicant's submission for RCE filed on Feb. 13, 2009 has been entered. Applicant has amended claims 1, 17, 30, 46. The applicant's amendment and remark have been entered. However, upon further consideration, Examiner maintains the rejection based on the previously cited prior art. See detail rejection above.

Regarding to applicant's argument to claims 1 and 17, have been fully considered but they are not persuasive.

Applicant argued, "nowhere do the cited portions of Dulude compare the first biometric data and the first transaction data against second biometric data and second transaction data". However, the limitation presented in the remark is not stated in the claimed language. The Applicant is reminded that presented arguments in the remark is not considered unless stated clearly in the claim language. In this instance the claimed language recites, *comparing the second processed data to the first processed data*. Dulude teaches comparing the second processed data (i.e. the second hashed value) to the first processed data (i.e. the first hashed value) as shown in Fig. 5 [component 80].



[col. 7 lines 15-16, "The first and second hash values are then compared by a first classifier 80"].

Further, claim limitation is not clarify the distinguish between the first and second values (first biometric data, first personal key and second biometric data, second personal key). Therefore, a biometric data entered by the user using the transaction biometric input device, is considered as a first biometric data and a biometric data received over a network, is considered as a second biometric data. Therefore, it meets the claim limitation. Further, Krawetz teaches comparing the check signature to the verification signature as shown in Fig. 3 [component 322, 324]. The signature data is considered as a processed data since it generates using the cryptographic algorithm. Further, Krawetz teaches discarding the identifier and the unencrypted data prior to any comparison [Fig. 3 component 311 – discard identifier and unencrypted data, 322, 324 – comparison i.e. prior to comparison]. Therefore, it meets the claim limitation. In this case, the combination of Dulude and Krawetz teaches the claim subject matter and the combination is sufficient because one of ordinary skill in the art at the time the invention was made would be motivated to combine Krawetz and Dulude to protect the database of the server against susceptible to loss or theft of the data associated with a user [Krawetz, paragraph 0003, 0006]. Furthermore, the examiner recognizes that obviousness can also be established by combining or modifying the teaching of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to on of ordinary skill in the art. See *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ 2nd 1941 (Fed. Cir 1992).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ferren et al (US 7047418) – Imaging method and device using biometric information and operator authentication

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/N. P./

Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435